

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representation of
The original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.

<p>(51) Classification internationale des brevets ⁶ : H04N 1/44</p>	<p>A1</p>	<p>(11) Numéro de publication internationale: WO 98/21880</p> <p>(43) Date de publication internationale: 22 mai 1998 (22.05.98)</p>
<p>(21) Numéro de la demande internationale: PCT/FR97/01686</p> <p>(22) Date de dépôt international: 25 septembre 1997 (25.09.97)</p> <p>(30) Données relatives à la priorité: 96/13916 8 novembre 1996 (08.11.96) FR</p> <p>(71) Déposant (pour tous les Etats désignés sauf US): FINTEL S.A. [FR/FR]; 87, boulevard Haussmann, F-75008 Paris (FR).</p> <p>(72) Inventeurs; et (75) Inventeurs/Déposants (US seulement): ROSSET, Franck [FR/FR]; 96, boulevard Beaumarchais, F-75011 Paris (FR). GAYET, Alain [FR/FR]; 13, place des Dominos, F-92400 Courbevoie (FR). MOULIN, Jean [FR/FR]; 5, avenue de Beauséjour, F-92210 Draveil (FR).</p> <p>(74) Mandataire: VIDON, Patrice; Cabinet Patrice Vidon, Im- meuble Germanium, 80, avenue des Buttes-de-Coësmes, F-35700 Rennes (FR).</p>		<p>(81) Etats désignés: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, brevet ARIPO (GH, KE, LS, MW, SD, SZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).</p> <p>Publiée Avec rapport de recherche internationale.</p>

A diagram illustrating a mobile communication system. On the left, a stick figure (11) holds a mobile phone (10) and a small device (14). A cable (13) connects the phone to a base station (16). The base station is connected to a central unit (15) via a cable (17). The central unit is connected to a printer (162) and a computer (161) via cables (19) and (18) respectively. The computer is connected to a server rack (21) via a cable (26). The server rack consists of multiple units (23, 24, 25, 26, 28). A cable (30) connects the server rack to a storage unit (41). A stick figure (40) is shown interacting with the storage unit.

L'invention concerne un procédé et un système permettant de transmettre une télécopie de manière sûre entre un émetteur émettant la télécopie et au moins un récepteur (11) recevant la télécopie (162) au moyen d'un télécopieur (161) associée à un équipement téléphonique (16). Les télécopies (162) sont acheminées entre émetteur et récepteur par un réseau de communication (15) via un centre de gestion des télécopies (30). Le centre de gestion des télécopies (30) met à la disposition du récepteur (11) une carte (10), au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque carte récepteur. Cette carte (10) émet de brefs signaux acoustiques d'identification, de type DTMF, cryptés au moins en partie, variant à chaque opération, lorsqu'elle est actionnée (14) par le récepteur (11). Les signaux reçus par le microphone (17) de l'équipement téléphonique (16) sont transmis par le réseau de communication (15) aux services informatiques (18) du centre de gestion des télécopies (30). Les signaux transmis et les données d'identification du récepteur et de la carte détenues (23) par les services informatiques (18) sont traités (24) et comparés (25) électroniquement par le service informatique (18) du centre de gestion des télécopies (30). En cas de coïncidence, le centre de gestion des télécopies (30) émet, à destination du télécopieur (161) du récepteur (11), la télécopie (162) qui lui est destinée par l'émetteur.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave	TM	Turkménistan
BF	Burkina Faso	GR	Grèce		de Macédoine	TR	Turquie
BG	Bulgarie	HU	Hongrie	ML	Mali	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MN	Mongolie	UA	Ukraine
BR	Brésil	IL	Israël	MR	Mauritanie	UG	Ouganda
BY	Bélarus	IS	Islande	MW	Malawi	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	MX	Mexique	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Pays-Bas	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NO	Norvège	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire	NZ	Nouvelle-Zélande		
CM	Cameroun		démocratique de Corée	PL	Pologne		
CN	Chine	KR	République de Corée	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Roumanie		
CZ	République tchèque	LC	Sainte-Lucie	RU	Fédération de Russie		
DE	Allemagne	LI	Liechtenstein	SD	Soudan		
DK	Danemark	LK	Sri Lanka	SE	Suède		
EE	Estonie	LR	Libéria	SG	Singapour		

Procédé et système pour sécuriser la transmission des télécopies au moyen d'une carte d'identification

Le domaine de l'invention est celui des procédés et des systèmes de transmission des télécopies. Pour plus de clarté les personnes désirant échanger une télécopie seront désignées, dans la suite du texte, respectivement sous les noms de "récepteur" et "d'émetteur".

Plus précisément l'invention concerne un procédé et un système permettant de transmettre une télécopie de manière sûre entre un émetteur émettant la télécopie et au moins un récepteur recevant la télécopie au moyen d'un télécopieur associé à un équipement téléphonique (ou à un terminal émulant cette fonction), les télécopies étant acheminées entre émetteur et récepteur par un réseau de communication via un centre de gestion des télécopies.

L'invention concerne également un procédé et un système permettant de transmettre une télécopie de manière sûre entre au moins deux personnes, l'une, l'émetteur, émettant la télécopie au moyen d'un premier télécopieur associé à un premier équipement téléphonique (ou à un premier terminal émulant cette fonction), l'autre, le récepteur, recevant la télécopie au moyen d'un second télécopieur associé à un second équipement téléphonique (ou à un second terminal émulant cette fonction), les télécopies étant acheminées par un réseau de communication via un centre de gestion des télécopies échangées entre émetteur et récepteur.

Certains prestataires de service peuvent être conduits à émettre des télécopies à usage de leurs abonnés ou de leurs clients (compte bancaire ou financier, rubriques d'informations personnalisées ou non, prévisions météorologiques locales, informations municipales, etc.) dont il convient d'éviter qu'elles ne parviennent à des personnes non-habilitées ou n'ayant pas acquitté leur abonnement. De même, de nombreuses entreprises (services du personnel, services financiers, services commerciaux, unités décentralisées) ainsi que les professions libérales (avocats, notaires, experts-comptables, etc.) sont conduites à échanger des télécopies contenant des informations confidentielles qu'ils ne souhaitent pas voir circuler entre les mains de tiers.

Le problème posé est d'empêcher un tiers mal intentionné d'accéder au centre de gestion

des télécopies sans y être autorisé, sans acquitter les droits correspondants.

Pour résoudre ce problème il a été proposé d'utiliser des clés d'accès que l'émetteur ou le récepteur génère au moyen d'un terminal multimédia ou au moyen d'équipements téléphoniques périphériques. Ces solutions, outre leur coût, sont peu pratiques et longues à mettre en oeuvre. En fait, le problème posé ne peut être effectivement résolu que si on sait résoudre simultanément un autre problème : concevoir un procédé et un système commode d'utilisation, rapide à mettre en oeuvre et économique. En effet, dès lors que l'on s'adresse à un large public, la facilité d'utilisation et les gains de temps deviennent des problèmes majeurs qui ne peuvent pas être ignorés.

Il a été proposé (document WO 96 04741 au nom de Andrew MARK) d'utiliser une carte émettant des signaux acoustiques, cryptés, de type DTMF, pour composer des numéros téléphoniques. Ainsi, le porteur d'une telle carte, en accouplant celle-ci au microphone du combiné téléphonique, transfère automatiquement ses identifiants. Comme ces identifiants sont chiffrés, on peut penser qu'un tiers ne sera pas en mesure d'en comprendre le contenu. La solution de A. MARK, concerne donc un tout autre secteur technique que celui de la transmission sécurisée des télécopies entre un émetteur et un récepteur via un centre de gestion des télécopies. Au surplus, l'enregistrement des signaux émis par la carte A. MARK reste possible et un fraudeur muni d'un tel enregistrement peut se substituer au bénéficiaire de la carte. La solution de A. MARK, ne permet donc pas d'empêcher un utilisateur mal intentionné d'accéder, sans y être autorisé, aux services offerts par le centre de gestion des télécopies.

Les objectifs visés par la présente invention sont atteints et les problèmes que posent les techniques selon l'art antérieur sont résolus, selon l'invention, à l'aide des procédés ci-après décrits.

Dans le cas d'une transmission de télécopies par un émetteur à une pluralité de récepteurs, le procédé selon l'invention comprend les étapes suivantes :

- le centre de gestion des télécopies met à la disposition du récepteur une carte, au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque carte et chaque récepteur,

- la dite carte, émet de brefs signaux acoustiques d'identification, de type DTMF, cryptés

au moins en partie, variant à chaque opération, lorsqu'elle est actionnée par le récepteur,

Le dit procédé comprend en outre les étapes suivantes :

- le récepteur actionne sa carte de telle sorte qu'elle émette des signaux acoustiques d'identification,

5 - les signaux reçus par le microphone de l'équipement téléphonique sont transmis via le réseau de communication et reçus par le service informatique du centre de gestion des télécopies,

10 - les signaux transmis et les données d'identification de l'émetteur et de la carte détenues par le service informatique sont traités et comparés électroniquement par le service informatique du centre de gestion des télécopies,

- en cas de coïncidence, le centre de gestion des télécopies, émet à destination du télécopieur du récepteur, la télécopie qui lui est destinée par l'émetteur.

15 Dans le cas d'une transmission de télécopies entre une pluralité d'émetteurs et de récepteurs, l'émetteur émet la télécopie au moyen d'un premier télécopieur associé à un premier équipement téléphonique (ou à un premier terminal émulant cette fonction), le récepteur reçoit la télécopie au moyen d'un second télécopieur associé à un second équipement téléphonique (ou à un second terminal émulant cette fonction). Les télécopies sont acheminées par un réseau de communication via un centre de gestion des télécopies.

Le procédé selon l'invention comprend les étapes suivantes :

20 - le centre de gestion des télécopies met à la disposition de l'émetteur et du récepteur une carte, au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque émetteur et chaque récepteur,

25 - les dites cartes, émettent de brefs signaux acoustiques d'identification, de type DTMF, cryptés au moins en partie, variant à chaque opération, lorsqu'elles sont actionnées par l'émetteur ou le récepteur,

- les dits signaux acoustiques d'identification sont reçus par le microphone de l'équipement téléphonique (ou du terminal émulant cette fonction) et sont convertis en signaux électroniques, avant d'être transmis par le réseau de communication au service informatique du centre de gestion des télécopies.

30 Le procédé comprend en outre les étapes suivantes :

- l'émetteur actionne sa carte de telle sorte qu'elle émette des signaux acoustiques d'identification,

- les signaux, reçus par le microphone du dit premier équipement téléphonique et transmis par le réseau de communication ainsi que les données d'identification de l'émetteur et de la carte détenues par le service informatique, sont traités et comparés électroniquement par le service informatique du centre de gestion des télécopies,

- en cas de coïncidence, la télécopie émise par l'émetteur au moyen du télécopieur est stockée par le centre de gestion des télécopies,

- le récepteur actionne sa carte de telle sorte qu'elle émette des signaux acoustiques d'identification,

- les signaux, reçus par le microphone de l'équipement téléphonique du récepteur et transmis par le réseau de communication ainsi que les données d'identification du récepteur et de la carte détenues par le service informatique, sont traités et comparés électroniquement par le service informatique du centre de gestion des télécopies,

- en cas de coïncidence, le centre de gestion des télécopies émet, à destination du télécopieur du récepteur, la télécopie stockée par le centre de gestion des télécopies.

Ainsi, grâce à ce procédé, le centre de gestion des télécopies peut vérifier que l'émetteur et/ou le récepteur disposent bien d'une carte authentique et non d'un leurre informatique.

Il a pu également identifier le titulaire de la carte comme étant une personne habilitée à émettre et/ou recevoir la copie qui lui est destinée. Par ailleurs, les fraudeurs n'ont plus la possibilité de dérober les données d'identification puisque celles-ci sont transmises automatiquement sous une forme cryptée. En outre, l'enregistrement, sous quelque forme que ce soit, des signaux acoustiques ne sera d'aucune utilité à un fraudeur pour se faire identifier par le centre de gestion des télécopies. En effet, les signaux acoustiques d'identification varient à chaque opération. C'est-à-dire chaque fois que la carte est actionnée.

De préférence la dite carte :

- décompte en outre le nombre de fois $C(p,n)$ où elle est actionnée,

- émet des signaux acoustiques représentatifs du nombre de fois $C(p,n)$ où elle a été actionnée,

- crypte les signaux acoustiques en fonction du nombre de fois $C(p,n)$ où elle a été actionnée.

De préférence également, les moyens informatiques du service informatique traitant et comparant électroniquement les signaux transmis et les données d'identification de l'émetteur ou du récepteur et des cartes,

- mémorisent le nombre de fois $C(p,m)$ où la carte a été actionnée lors de dernière opération validée,

- comparent le nombre de fois $C(p,n)$ où la carte a été actionnée, lors de l'opération en cours, avec le nombre de fois mémorisé $N1$,

- rejettent l'opération en cours si $C(p,n)$ est inférieur ou égal à $C(p,m)$ et poursuivent la vérification de l'opération en cours si $C(p,n)$ est supérieur à $C(p,m)$,

- recalculent les signaux électroniques $S'(p,n)$ en fonction des données d'identification et du nombre de fois $C(p,n)$ où la carte a été actionnée, lors de l'opération en cours, puis les comparent aux signaux électroniques $S(p,n)$ transmis.

Afin d'augmenter la sécurité du procédé, dans une variante de réalisation, le procédé comprend en outre l'étape suivante : l'émetteur et/ou le récepteur émettent, au moyen d'un clavier associé à l'équipement téléphonique et/ou à la carte, un code confidentiel. Après transmission au service informatique du centre de gestion des télécopies, par le réseau de communication, ce code confidentiel est traité et comparé au code confidentiel personnel de l'émetteur et/ou du récepteur détenu par le service informatique du centre de gestion de télécopies. Ainsi, le centre de gestion des télécopies peut vérifier que l'émetteur et/ou le récepteur est bien la personne habilitée à recevoir la télécopie confidentielle. Une carte volée ne peut pas être utilisée par le fraudeur.

Avantageusement, afin d'informer le récepteur qu'une télécopie est tenue à sa disposition, le centre de gestion des télécopies émet à l'attention du récepteur un avis de mise à disposition d'une télécopie confidentielle.

Le procédé peut également être tel que le centre de gestion des télécopies émet un avis de relève de la télécopie vers l'émetteur.

L'invention concerne aussi un système permettant de transmettre une télécopie de manière sûre entre un émetteur émettant la télécopie et au moins un récepteur recevant la télécopie

au moyen d'un télécopieur associé à un équipement téléphonique (ou à un terminal émulant cette fonction), les télécopies étant acheminées entre émetteur et récepteur par un réseau de communication via un centre de gestion des télécopies.

Ce système a pour caractéristique de comprendre les moyens de mise en oeuvre du procédé ci-dessus défini et de ses variantes de réalisation.

Plus particulièrement.

- Le système selon l'invention comprend au moins une carte à l'usage du récepteur, au format carte de crédit, personnalisée par des identifiants spécifiques à chaque carte et à chaque récepteur. La dite carte comporte des moyens d'émission de brefs signaux acoustiques d'identification, de type DTMF, actionnés par le récepteur, au moyen d'un élément accessible de l'extérieur de la carte. La dite carte comporte en outre des moyens de cryptage permettant de crypter au moins en partie et de varier les signaux acoustiques chaque fois que la carte est actionnée.

- Le système selon l'invention comprend un équipement téléphonique (ou tout terminal émulant cette fonction) comprenant un microphone destiné à recevoir et transformer les signaux acoustiques reçus en des signaux électroniques transmis par le réseau de communication au service informatique du centre de gestion des télécopies.

- Le système selon l'invention comprend également des moyens informatiques, associés au service informatique du centre de gestion des télécopies, connectés au réseau de communication, les dits moyens informatiques comprenant :

- une base de données contenant les références de chaque carte et de chaque récepteur et leurs données d'identification,
- des moyens de traitement et des moyens de comparaison des signaux électroniques et des données d'identification contenues dans la base de données,
- des moyens d'émission émettant, en cas de coïncidence, à destination du télécopieur du récepteur, la télécopie qui lui est destinée par l'émetteur.

L'invention concerne également un système permettant de transmettre une télécopie de manière sûre entre au moins deux personnes, l'une l'émetteur émettant la télécopie au moyen d'un premier télécopieur associé à un premier équipement téléphonique (ou à un premier terminal émulant cette fonction), l'autre le récepteur recevant la télécopie au

moyen d'un second télécopieur associé à un second équipement téléphonique (ou à un second terminal émulant cette fonction). Les télécopies sont acheminées par un réseau de communication via un centre de gestion des télécopies échangées entre émetteur et récepteur.

5 Le système comprend au moins deux cartes, l'une à l'usage du récepteur, l'autre à l'usage de l'émetteur. Ces cartes, au format carte de crédit, sont personnalisée par des identifiants spécifiques à chaque carte et à chaque émetteur ou récepteur. Chaque carte comporte des moyens d'émission de brefs signaux acoustiques d'identification, de type DTMF, actionnés par l'émetteur ou le récepteur, au moyen d'un élément accessible de l'extérieur
10 de la carte. Chaque carte comporte en outre des moyens de cryptage permettant de crypter au moins en partie et de varier les signaux acoustiques chaque fois que la carte est actionnée.

Le système est tel que le premier et le second équipement téléphonique (ou le premier ou le second terminal émulant cette fonction) comprennent un microphone destiné à recevoir
15 et transformer les signaux acoustiques reçus en des signaux électroniques transmis par le réseau de communication au service informatique du centre de gestion des télécopies.

Le système comprend en outre des moyens informatiques, associés au service informatique du centre de gestion des télécopies, connectés au réseau de communication. Ces moyens informatiques comprennent :

20 - une base de données contenant les références de chaque carte et de chaque récepteur ou émetteur et leurs données d'identification,
- des moyens de traitement et des moyens de comparaison des signaux électroniques et des données d'identification contenues dans la base de données,
- des moyens de stockage stockant, en cas de validation des identifiants de la carte de
25 l'émetteur, la télécopie émise par le premier télécopieur,
- des moyens d'émission émettant la télécopie à destination du télécopieur du récepteur, en cas de validation des identifiants de la carte du récepteur.

Ainsi, grâce à ce système, le centre de gestion des télécopies peut vérifier que l'émetteur et/ou le récepteur disposent bien d'une carte authentique et non d'un leurre informatique.

30 Il a pu également identifier le titulaire de la carte comme étant une personne habilitée à

recevoir la copie qui lui est destinée. Par ailleurs, les fraudeurs n'ont pas la possibilité de dérober les données d'identification puisque celles-ci sont transmises automatiquement sous une forme cryptée. En outre, l'enregistrement, sous quelque forme que ce soit, des signaux acoustiques ne sera d'aucune utilité à un fraudeur pour se faire identifier par le centre de gestion des télécopies. En effet, les signaux acoustiques d'identification varient à chaque opération. C'est-à-dire chaque fois que la carte est actionnée.

De préférence la dite carte comporte en outre :

- un compteur incrémental interconnecté aux moyens d'émission et aux moyens de cryptage s'incrémentant d'au moins une unité chaque fois que la carte est actionnée.

De sorte que l'état du compteur incrémental est émis à destination des moyens informatiques et que les signaux acoustiques sont cryptés en fonction de l'état du compteur incrémental.

De préférence également les dits moyens informatiques comportent en outre :

- des moyens de mémorisation de l'état $C(p,m)$ du compteur incrémental lors de la dernière opération validée,

- des moyens de comparaison de l'état $C(p,n)$ du compteur incrémental émis lors de l'opération en cours avec l'état $C(p,m)$ du compteur incrémental mémorisé.

De sorte que la vérification de l'opération en cours est rejetée si $C(p,n)$ est inférieur ou égal à $C(p,m)$ et est poursuivie si $C(p,n)$ est strictement supérieur à $C(p,m)$.

De préférence également les dits moyens de traitement et les dits moyens de comparaison des signaux électroniques et des données d'identification contenues dans la base de données comportent des moyens permettant de recalculer les signaux électroniques en fonction de l'état $C(p,n)$ du compteur incrémental et des données d'identification puis de les comparer aux signaux électroniques transmis.

Afin d'augmenter la sécurité du système, dans une variante de réalisation, les dits moyens informatiques comprenant en outre:

- des seconds moyens de comparaison d'un code confidentiel personnel au récepteur, contenu dans la base de données, à un code confidentiel personnel,

- émis par le récepteur, au moyen d'un clavier associé à l'équipement téléphonique ou à la carte du récepteur et,

- transmis aux moyens informatiques du centre de gestion des télécopies, par le réseau de communication.

Ainsi, le centre de gestion de télécopies peut vérifier que le récepteur est bien la personne habilitée à entrer en relation avec ses services. Une carte volée ne peut pas être utilisée par le voleur faute de connaître le code confidentiel.

Avantageusement, afin d'informer le récepteur qu'une télécopie est tenue à sa disposition, le centre de gestion des télécopies comporte des moyens délivrant, à destination du récepteur, un avis de mise à disposition de la télécopie stockée.

Le système peut également être tel que le centre de gestion des télécopies comporte en outre des moyens d'émission d'un avis de relève de la télécopie, vers l'émetteur.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description des variantes de réalisation de l'invention, données à titre d'exemple indicatif et non limitatif. Les figures représentent :

- figure 1 : le système et le procédé selon l'invention dans le cas d'une transmission de télécopies par un émetteur à une pluralité de récepteurs,

- figure 2 le système et le procédé selon l'invention dans le cas d'une transmission de télécopies entre une pluralité d'émetteurs et de récepteurs.

- figure 3 la carte sous la forme de bloc diagramme,

- figure 4 l'algorithme de vérification de l'authenticité du signal transmis.

On va maintenant décrire la figure 1. Le système et le procédé selon l'invention permettent au récepteur 11 de recevoir d'une manière sûre et rapide, au moyen d'un télécopieur 161 associé à un combiné téléphonique 16 comportant un microphone 17, une télécopie 162 que le centre de gestion des télécopies 30 d'un prestataire de service 40 émet à destination des récepteurs 11 abonnés ou clients de ses services 41 (services météorologiques, services boursiers personnalisés, etc.). Le combiné téléphonique 16 et le télécopieur du récepteur, situés à distance des services informatiques 18 du centre de gestion des télécopies 30, sont connectés aux services informatiques 18 via un réseau de communication 15.

Le système comprend une carte 10, au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque carte et pour chaque récepteur. Cette carte est mise à

la disposition des récepteurs par le centre de gestion des télécopies 30 ou les prestataires de service 40, 41. La carte 10 comporte des moyens 13 d'émission, notamment un haut-parleur 13, émettant de brefs signaux acoustiques d'identification 20, de type DTMF. Ces signaux 20 sont émis lorsque les moyens d'émission 13 sont actionnés par le récepteur au moyen d'un élément 14 accessible de l'extérieur de la carte (non visible sur la figure 1 car
5 situé sur l'autre côté de la carte). Ces moyens d'émission 13 sont excités par un générateur de signaux DTMF 99, contrôlé par un microprocesseur 104 alimenté par une pile 106 et piloté par un résonateur 107. Le microprocesseur 104 contenu dans la carte comporte des moyens de cryptage 103 permettant de crypter, au moins en partie, les
10 signaux acoustiques 20, comportant un algorithme de cryptage 108 et des identifiants 109 spécifiques pour chaque carte 10 et pour chaque client 11, notamment la clé secrète 250 utilisée par algorithme de cryptage 108. Les signaux acoustiques 20 sont reçus par le microphone 17 du combiné téléphonique, contre lequel le client accole la carte 10. Le système comprend également des moyens de transmission 19 des signaux acoustiques
15 20, situés dans le combiné téléphonique 16. Ces moyens de transmission 19 transmettent à distance les signaux, après traitement et conversion en signaux électroniques, via le réseau de communication 15.

Le système comprend également des moyens informatiques 21, dépendants des services informatiques 18 du centre de gestion des télécopies 30. Ces moyens informatiques sont
20 connectés au réseau de communication 15 et situés à distance des combinés téléphoniques 16 et des télécopieurs 161.

Ces moyens informatiques 21 comprennent eux-mêmes :

- une base de données 23 contenant les références de chaque carte et de chaque récepteur et leurs données d'identification,
- 25 - des moyens de traitement 24 et des moyens de comparaison 25 des signaux électroniques et des données d'identification contenues dans la base de données,
- des moyens d'émission de télécopie 28 émettant, en cas de comparaison positive, à destination du télécopieur 161 du récepteur 11, la télécopie 162 qui lui est destinée par l'émetteur.

30 La séquence d'utilisation est donc la suivante :

- Avec le clavier 164 de son télécopieur, le récepteur 11 compose le numéro de téléphone du centre de gestion des télécopies. Dès le décroché, une voix l'invite à s'identifier grâce à sa carte 10.

- Le récepteur 11 utilise sa carte 10 avec le microphone 17 du combiné téléphonique 16 associé au télécopieur 161. Il est alors immédiatement identifié et sa carte 10 est authentifiée.

- Il entend alors son télécopieur 161 entrer en relation avec le centre de gestion des télécopies 30. Il peut alors raccrocher, son télécopieur 161 ayant pris la ligne de communication 15, puis toujours au sein de la même communication téléphonique, il reçoit la télécopie 162 contenant les informations attendues.

De préférence, ainsi qu'on va le décrire en se référant aux figures 3 et 4, le microprocesseur 104 et les moyens de cryptage 103 sont conçus de telle sorte que le signal acoustique 20 varie à chaque opération. En effet, crypter un code d'identification c'est le transformer en une suite d'informations, incompréhensibles pour tout un chacun, et que, seul le titulaire de la clef de cryptage, pourra décrypter. Mais cela n'empêche absolument pas la copie du code d'identification crypté, soit au cours de sa transmission acoustique (magnétophone), soit par piratage de la ligne téléphonique. Cette copie utilisée indûment par un fraudeur, sera traitée par le système récepteur comme ayant toutes les caractéristiques de l'original, puis interprétée afin de vérifier les identifiants de la carte.

Le problème posé est donc le suivant : comment rendre impossible toute tentative de reproduction ? Il sera ci-après décrit différentes variantes de réalisation du moyen général qui permet de faire la distinction entre l'original et la copie, lors de l'analyse du signal crypté reçu par les moyens informatiques 21, en insérant un élément distinctif dans le signal 20 du type DTMF émis par la carte 10.

L'une de variantes consiste à utiliser une fonction dite d'horodatage (par exemple, ainsi qu'elle a été décrite dans le brevet US n° 4 998 279). Cette fonction d'horodatage exploite le paramètre "temps" qui évolue en permanence. La "copie" se trouve ainsi en retard, quand elle est émise. Une telle solution nécessite une synchronisation entre les moyens d'émission 13 et les moyens informatiques 21. Pour cela, tous les deux doivent disposer d'une "base de temps" et d'un "étalon de fréquence". Ces deux bases de temps ont leur

précision propre et leur dérive propre. Il en résulte qu'elles se désynchronisent lentement, mais progressivement. Pour remédier à cette difficulté technique, une certaine dérive est tolérée entre les bases de temps des moyens d'émission 13 et des moyens informatiques 21. Plus cette dérive est importante, plus l'incertitude augmente sur la "validité" de l'information reçue et plus augmente le risque de fraude. Ainsi si une dérive de une minute est tolérée, toute copie illicite de l'émission du signal crypté, et réutilisée frauduleusement dans les 30 secondes qui suivent, sera perçue comme valide par le système d'analyse des moyens informatiques 21.

Une autre variante consiste à utiliser des listes incrémentales (par exemple, ainsi qu'elle a été décrite dans le brevet US n° 4 928 098). Le dispositif d'émission et celui de réception possèdent la liste ordonnée des cryptages successifs du code d'identification ou bien disposent des algorithmes permettant de les établir au fur et à mesure. A un instant donné, les moyens informatiques 21 sont en attente du résultat crypté $C(n)$. S'ils reçoivent effectivement le message $C(n)$, il valide l'opération. Mais les moyens informatiques 21 peuvent recevoir un message différent, en effet l'utilisateur de la carte peut avoir actionné plusieurs fois les moyens d'émission 13 de celle-ci, par jeu, par maladresse, de sorte que la carte est dans la situation d'émettre le résultat crypté $C(n+p)$ lors de sa prochaine utilisation avec les moyens informatiques 21. Si les moyens informatiques 21 reçoivent un message différent, ils cherchent en avant, dans la liste de résultats cryptés successifs, s'il existe un message $C(n+p)$ identique à celui reçu. Pour lever l'ambiguïté "est-ce un message authentique émis par l'émetteur ?" ou "est-ce un message frauduleux ?", la solution consiste à demander ou à attendre l'émission suivante. Si celui-ci est identique à $C(n+p+1)$, le système valide alors le message et se place dans l'attente de la prochaine émission, dans l'état $C(n+p+2)$. Si celui-ci est différent, le message n'est pas validé et le système d'analyse reste en attente du message $C(n)$. Une telle variante de réalisation n'est pas très ergonomique puisqu'elle oblige le titulaire de la carte à actionner plusieurs fois celle-ci.

Selon une variante de réalisation préférentielle, pour distinguer le signal original de sa copie, le microprocesseur 104 embarqué dans la carte 10 comporte un compteur incrémental 105. A chaque usage de la carte, le compteur incrémental 105 s'incrémente

d'une ou de plusieurs unités. Bien évidemment, telle une roue à cliquet, celui-ci ne peut revenir en arrière, il ne peut qu'avancer à chaque usage.

Dans le cas de cette variante de réalisation, l'état $C(p,n)$ 242 du compteur 105 entre dans le calcul du message crypté 244 émis par les moyens d'émission 13. La partie codée $S(p,n)$ 241 est calculée par l'algorithme 108 (dont l'équivalent 247 est mémorisé dans les moyens informatiques 21 au moyen de la clé secrète 250 spécifique à chaque carte et de l'état $C(p,n)$ 242 du compteur 105. La carte 10 émet, en plus du numéro d'identification $I(p)$ 240 de la carte et du code d'identification crypté $S(p,n)$ 241, l'état $C(p,n)$ 242 de son compteur incrémental 105 à chaque émission. Les moyens informatiques 21 mémorisent 230, dans la base de données 23, l'état $C(p,n)$ 242 du compteur incrémental 105 lors de la dernière opération validée. Ainsi, à chaque réception de message 244, les moyens de comparaison 25 des moyens informatiques 21 peuvent comparer 245 l'information reçue relative à l'état $C(p,n)$ 242 du compteur 105, à la précédente information reçue $C(p,m)$ 246 et gardée en mémoire 230, 23.

a) - Si l'état $C(p,n)$ 242 du compteur 105 (fig. 2) exprimé dans le message 244 est strictement supérieur ($n > m$) à celui $C(p,m)$ 246 précédemment reçu, alors le message 244 est accepté et l'analyse se poursuit.

b)- Si l'état $C(p,n)$ 242 du compteur 105 exprimé dans le message 244 est inférieur ou égal ($n \leq m$) à celui $C(p,m)$ 246 précédemment reçu, alors le message est refusé. Le message reçu ne peut être qu'une copie antérieurement effectuée ou un leurre informatique.

Si les conditions définies au point a) ci-dessus sont réunies, les moyens informatiques 21 permettent de lire la partie fixe $I(p)$ 240 et de rechercher dans leur propre base de données 23, 230 la clé secrète correspondante de la carte. Les moyens de calcul 239 des moyens de traitement 24 peuvent alors au moyen l'algorithme 247, de l'état du compteur $C(p,n)$ 242 et de la clé secrète $Clé(p)$ 250, procéder au calcul du code crypté attendu par les moyens informatiques 21. Le code crypté $S'(p,n)$ 248 ainsi calculé est comparé 249 à celui effectivement reçu $S(p,n)$ 241, par les moyens de comparaison 25. Ce procédé et ces moyens permettent donc de valider ou d'invalider le message 244, sans qu'il soit nécessaire à l'utilisateur de la carte d'actionner plusieurs fois celle-ci, comme cela est le

cas dans la variante de réalisation ci-dessus décrite.

L'existence au sein de la carte 10 d'un compteur incrémental 105 permet, sans coût supplémentaire, de fixer, au moment de la programmation individuelle de la carte, le nombre maximum de fois où la carte peut-être utilisée. Une fois ce maximum atteint, celle-ci n'émet plus de message cohérent et est donc refusée par les moyens informatiques 21.

La trame 244 émise contient, pour une carte donnée (p),

- une partie fixe I(p) 240 (le numéro d'identification de la carte),
- une partie variable incrémentale C(p,n) 242 (l'état du compteur),
- une partie variable S(p,n) 241 apparemment aléatoire (le résultat d'un algorithme de cryptage 108 sur la clé secrète 250 propre à cette carte (p)).

La trame émise :

- est toujours différente d'une carte à l'autre,
- est, pour une carte donnée, toujours différente à chaque émission.

Les moyens informatiques 21 permettent, pour une carte donnée (p), de :

- lire la partie fixe I(p) 240 (le numéro d'identification de la carte),
- rechercher dans leur propre base de données 23 la clé secrète 250 de cette carte et le dernier enregistrement reçu de l'état C(p,m) 246 du compteur 105 de cette carte,
- rejeter cette trame 244 si l'état du compteur C(p,n) 242 de l'opération en cours est inférieur ou égal à celui C(p,m) 246 précédemment reçu et de poursuivre la vérification de l'opération en cours si l'état C(p,n) 242 est strictement supérieur à celui C(p,m) 246 précédemment reçu,
- de "décrypter" le message 244 reçu et d'en valider le contenu, en le recalculant au moyen de l'algorithme de cryptage 247, de la clé spécifique 250 de cette carte et de l'état du compteur C(p,n) 242, puis en comparant le résultat de ce calcul au message reçu.

Ainsi, grâce à cette combinaison de moyens il est possible d'émettre, au moyen d'une carte ayant le format d'une carte de crédit, des fréquences acoustiques de type DTMF d'identification, recevables par le microphone d'un équipement relié au réseau téléphonique, et d'avoir la certitude de l'authenticité de la carte appelante et d'écarter ainsi tous les fraudeurs utilisant tout enregistrement sonore ou informatique ou tout leurre

informatique.

Afin d'augmenter la sécurité du système, dans la variante de réalisation représentée sur la figure 1, les moyens informatiques 21 comprennent en outre des seconds moyens de comparaison 26. Ces moyens de comparaison 26 permettent de comparer un code confidentiel personnel du récepteur, contenu dans la base de données 23, avec le code confidentiel émis par le récepteur. Ce code est émis au moyen d'un clavier 27 associé au combiné téléphonique 16 et/ou à la carte 10 et/ou au moyen du clavier 164 du télécopieur 161. Ce code est transmis aux moyens informatiques 21 du centre de gestion des télécopies, par le réseau de communication 15.

Ainsi, le centre de gestion des télécopies et les prestataires de service 40,41 ont l'assurance que le récepteur 11 est bien la personne habilitée à entrer en relation avec les services des prestataires de service. Une carte volée ne peut pas être utilisée par le voleur faute de connaître le code confidentiel.

On va maintenant décrire la figure 2 qui représente le système et le procédé selon l'invention dans le cas d'une transmission de télécopies entre une pluralité d'émetteurs et de récepteurs. En effet de nombreuses entreprises (services du personnel, services financiers, services commerciaux, unités décentralisées) ainsi que les professions libérales (avocats, notaires, experts-comptables, etc.) sont conduites à échanger des télécopies contenant des informations confidentielles qu'ils ne souhaitent pas voir circuler entre les mains de tiers.

Le système et le procédé selon l'invention permettent de transmettre une télécopie 162, 262 de manière sûre entre au moins deux personnes, l'une, l'émetteur 11, émettant la télécopie 162 au moyen d'un premier télécopieur 161 associé à un premier équipement téléphonique 16 (ou à un premier terminal émulant cette fonction), l'autre, le récepteur 111, recevant la télécopie 262 au moyen d'un second télécopieur 261 associé à un second équipement téléphonique 116 (ou à un second terminal émulant cette fonction).

Les télécopies sont acheminées par un réseau de communication 15 via un centre de gestion des télécopies 30 échangées entre émetteur 11 et récepteur 111.

Le système comprend au moins deux cartes 10 et 110, l'une 10 à l'usage de l'émetteur 11, l'autre 110 à l'usage du récepteur 111. Ces cartes sont mises à la disposition des

émetteurs et des récepteurs par le centre de gestion des télécopies 30 ou par un opérateur de télécommunication ou par un prestataire de service. Chaque carte est au format carte de crédit, et est personnalisée par des identifiants spécifiques à chaque carte et à chaque émetteur ou récepteur. Chaque carte comporte des moyens d'émission 13, 113 de brefs
5 signaux acoustiques d'identification 20, 120, de type DTMF, cryptés au moins en partie, lorsque les moyens d'émission 13, 113 sont actionnés par l'émetteur 11 ou le récepteur 111, au moyen d'un élément 14, 114 accessible de l'extérieur de la carte (non visible 2 sur la figure car situé sur l'autre côté de la carte).

Les signaux acoustiques 20, 120 sont reçus par les microphones 17, 117 des
10 équipements téléphoniques, contre lesquels l'émetteur et le récepteur accolent leur carte 10, 110. Le système comprend également des moyens de transmission 19, 119 des signaux acoustiques 20, 120, situés dans les équipements téléphoniques 16, 116. Ces moyens de transmission transmettent à distance les signaux électroniques, après traitement, via le réseau de communication 15. Le système comprend également des
15 moyens informatiques 21, dépendants des services informatiques 18 du centre de gestion des télécopies 30. Ces moyens informatiques sont connectés au réseau de communication 15 et situés à distance des équipements téléphoniques 16, 116 et des télécopieurs 161, 261.

Ces moyens informatiques 21 comprennent :

- 20 - une base de données 23 contenant les références de chaque carte et de chaque récepteur ou émetteur et leurs données d'identification,
- des moyens de traitement 24 et des moyens de comparaison 25 des signaux électroniques et des données d'identification contenues dans la base de données.
- des moyens de stockage 21a stockant, en cas de validation des identifiants de la carte de
25 l'émetteur 11, la télécopie émise par le premier télécopieur 161,
- des moyens de délivrance 21b délivrant, à destination du récepteur 11, un avis de mise à disposition 190 de la télécopie stockée,
- des moyens d'émission de télécopie 28 émettant, à destination du télécopieur 261 du
30 récepteur 111, en cas de validation des identifiants de la carte du récepteur 111, la télécopie 262 pour laquelle le centre de gestion des télécopies a délivré l'avis de mise à

disposition 190.

De préférence les moyens de cryptage de la carte et de décryptage des services informatiques sont conçus de telle sorte que le signal acoustique varie à chaque opération, ainsi que cela a été décrit ci-dessus, notamment en se référant aux figures 3 et 4.

5 La séquence d'utilisation est donc la suivante.

A l'émission :

- Avec le clavier 164 de son télécopieur ou le clavier 27 de son équipement téléphonique 16, l'émetteur 11 compose le numéro de téléphone du centre de gestion des télécopies 30. Dès le décroché, une voix l'invite à s'identifier grâce à sa carte 10.

10 - L'émetteur 11 utilise sa carte 10 avec le microphone 17 de l'équipement téléphonique 16 associé au télécopieur 161. Il est alors immédiatement identifié et sa carte 10 est authentifiée.

- Il est alors invité à taper le numéro de télécopie du récepteur. Si ce numéro figure dans la liste des correspondants autorisés, il entend alors son télécopieur 161 entrer en relation avec le centre de gestion des télécopies 30. Il peut alors raccrocher, son télécopieur 161 ayant pris la ligne de communication 15.

15 - La télécopie 162 arrive au centre de gestion des télécopies 30 où elle est stockée. Le centre de gestion des télécopies envoie alors un avis de mise à disposition 190 au récepteur 111 désigné.

20 A la réception :

- Le récepteur 111, ainsi averti, se présente auprès de son télécopieur 261. Il compose au moyen du clavier 127 de l'équipement téléphonique 116 associé à son télécopieur 261 le numéro du centre de gestion des télécopies. Dès le décroché, une voix l'invite à s'identifier grâce à sa carte.

25 - Le récepteur 111 utilise sa carte 110 avec le microphone 117 de l'équipement téléphonique 116. Le centre de gestion des télécopies 30 émet la télécopie qui est destinée au récepteur 111 ainsi identifié, après avoir invité le récepteur 111 à ne pas quitter le télécopieur 261.

30 Afin d'augmenter la sécurité du système, dans la variante de réalisation représentée sur la figure 2, les moyens informatiques 21 comprennent en outre des seconds moyens de

comparaison 26. Ces moyens de comparaison 26 permettent de comparer un code confidentiel personnel du récepteur et/ou de l'émetteur, contenu dans la base de données 23, avec le code confidentiel émis par le récepteur et/ ou l'émetteur. Ces codes sont émis au moyen des claviers 27, 127 associés aux équipements téléphoniques 16, 116 et/ou aux
5 cartes 10 110 et/ou au moyen des claviers 164, 264 des télécopieurs 161, 261. Ces codes sont transmis aux moyens informatiques 21 du centre de gestion des télécopies 30, par le réseau de communication 15.

Ainsi, le centre de gestion des télécopies 30 ainsi que l'émetteur et le récepteur ont l'assurance que la télécopie est bien échangée entre les personnes habilitées. Une carte
10 volée ne peut pas être utilisée par le voleur faute de connaître le code confidentiel.

Dans la variante de réalisation représentée sur la figure 2, le centre de gestion des télécopies 30 comprend en outre des moyens d'émission 29 d'un avis de relève 191 de la télécopie vers l'émetteur 11.

REVENDICATIONS

1. Procédé permettant de transmettre une télécopie de manière sûre entre un émetteur émettant la télécopie et au moins un récepteur (11 fig. 1) recevant la télécopie (162 fig. 1) au moyen d'un télécopieur (161 fig. 1) associé à un équipement téléphonique (16 fig. 1) (ou à un terminal émulant cette fonction), les télécopies étant acheminées entre émetteur et récepteur par un réseau de communication (15) via un centre de gestion des télécopies (30), le dit procédé étant tel que :

- le centre de gestion des télécopies (30) met à la disposition du récepteur (11 fig. 1) une carte (10 fig. 1), au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque carte et chaque récepteur,

- la dite carte (10 fig. 1) émet de brefs signaux acoustiques d'identification, de type DTMF, cryptés au moins en partie, variant à chaque opération, lorsqu'elle est actionnée (14 fig. 1) par le récepteur (11 fig. 1),

le dit procédé comprend les étapes suivantes :

- le récepteur (11 fig. 1) actionne (14 fig. 1) sa carte (10 fig. 1) de telle sorte qu'elle émette des signaux acoustiques (20 fig. 1) d'identification,

- les signaux reçus par le microphone (17 fig. 1) du dit équipement téléphonique (16 fig. 1) sont transmis via le réseau de communication (15 fig. 1) et reçus par le service informatique (18 fig. 1) du centre de gestion (30) des télécopies,

- les signaux transmis et les données d'identification de l'émetteur et de la carte détenues par le service informatique (18 fig. 1) sont traités (24) et comparés (25) électroniquement par le service informatique (18 fig. 1) du centre de gestion (30) des télécopies,

- de sorte qu'en cas de coïncidence, le centre de gestion des télécopies (30), émet à destination du télécopieur (161 fig. 1) du récepteur (11 fig. 1), la télécopie (162 fig. 1) qui lui est destinée par l'émetteur.

2. Procédé permettant de transmettre une télécopie de manière sûre entre au moins deux personnes, l'une l'émetteur (11 fig. 2) émettant la télécopie (162 fig. 2) au moyen d'un premier télécopieur (161 fig. 2) associé à un premier équipement téléphonique (16 fig. 2) (ou à un premier terminal émulant cette fonction), l'autre le récepteur (111 fig. 2) recevant la télécopie (262 fig. 2) au moyen d'un second télécopieur (261 fig. 2) associé à un

20,

second équipement téléphonique (116 fig. 2) (ou à un second terminal émulant cette fonction), les télécopies (162) étant acheminées par un réseau de communication (15) via un centre de gestion (30) des télécopies échangées entre émetteur (11) et récepteur (111),

- le centre de gestion (30) des télécopies met à la disposition de l'émetteur (11 fig. 2) et du récepteur (111 fig. 2) une carte (10,110 fig. 2), au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque émetteur (11 fig. 2) et chaque récepteur (111 fig. 2),

- la dite carte (10,110 fig. 2), émet de brefs signaux acoustiques d'identification, de type DTMF, cryptés au moins en partie, variant à chaque opération, lorsqu'elle est actionnée (14) par l'émetteur (11 fig. 2) ou le récepteur (111 fig. 2),

- les dits signaux acoustiques d'identification sont reçus par le microphone (17,117 fig. 2) de l'équipement téléphonique (ou du terminal émulant cette fonction) et sont convertis en signaux électroniques, avant d'être transmis par le réseau de communication (15) au service informatique (18) du centre de gestion (30) des télécopies,

le dit procédé comprend les étapes suivantes :

- l'émetteur (11 fig. 2) actionne (14 fig. 2) sa carte de telle sorte qu'elle émette des signaux acoustiques (20 fig. 2) d'identification,

- les signaux (20 fig. 2) reçus par le microphone (117 fig. 2) du dit premier équipement téléphonique (16 fig. 2) et transmis par le réseau de communication (15 fig. 2) ainsi que les données d'identification de l'émetteur et de la carte détenues par le service informatique (18 fig. 2) sont traités (24 fig. 2) et comparés (25 fig. 2) électroniquement par le service informatique (18 fig. 2) du centre de gestion (30 fig. 2) des télécopies,

- de sorte qu'en cas de coïncidence, la télécopie (162 fig. 2) émise par l'émetteur (11 fig. 2) au moyen du dit premier télécopieur (161 fig. 2) est stockée par le centre de gestion des télécopies (30),

- le récepteur (111 fig. 2) actionne sa carte (110 fig. 2) de telle sorte qu'elle émette des signaux acoustiques (120 fig. 2) d'identification,

- les signaux reçus par le microphone (117 fig. 2) du dit second équipement téléphonique (116 fig. 2) et transmis par le réseau de communication (15 fig. 2) ainsi que les données d'identification du récepteur et de la carte détenues par le service informatique

21,

(18 fig. 2) sont traités (24 fig. 2) et comparés (25 fig. 2) électroniquement par le service informatique (18 fig. 2) du centre de gestion (30 fig. 2) des télécopies,

- de sorte qu'en cas de coïncidence, le centre de gestion (30) des télécopies, émet à destination du second télécopieur (261 fig. 2) et du récepteur (111 fig. 2), la télécopie (262 fig. 2) stockée par le centre de gestion des télécopies.

3. Procédé selon les revendications 1 ou 2,

- la dite carte (10) :

* décompte (105) en outre le nombre de fois $C(p,n)$ (242) où elle est actionnée par l'élément (14),

* émet des signaux acoustiques (20) représentatifs du nombre de fois $C(p,n)$ (242) où elle a été actionnée,

* crypte (103) les signaux acoustiques en fonction du nombre de fois $C(p,n)$ (242) où elle a été actionnée,

- les moyens informatiques (21) du service informatique (18) traitant (24) et comparant (25) électroniquement les signaux transmis ainsi que les données d'identification de l'émetteur ou du récepteur et de la carte détenues (23) par le service informatique (18) du centre de gestion des télécopies,

* mémorisent (230) le nombre de fois $C(p,m)$ (246) où la carte a été actionnée lors de dernière opération validée,

* comparent (245) le nombre de fois $C(p,n)$ (242) où la carte a été actionnée, lors de l'opération en cours, avec le nombre de fois mémorisé $C(p,m)$ (246),

* rejettent l'opération en cours si $C(p,n)$ (242) est inférieur ou égal à $C(p,m)$ (246) et poursuivent la vérification de l'opération en cours si $C(p,n)$ (242) est supérieur à $C(p,m)$ (246),

* recalculent (239) les signaux électroniques $S'(p,n)$ (248) en fonction des données d'identification et du nombre de fois $C(p,n)$ (242) où la carte a été actionnée, lors de l'opération en cours, puis les comparent (249) aux signaux électroniques transmis $S(p,n)$ (241).

4. Procédé selon les revendications 1, 2, ou 3, comprenant en outre l'étape suivante :

- l'émetteur et/ou le récepteur émet, au moyen d'un clavier (27,127) associé au premier

et/ou au second équipement téléphonique (16,116), un code confidentiel personnel ; après transmission au service informatique (18) du centre de gestion (30) des télécopies, via le réseau de communication (15), ce code confidentiel personnel est traité et comparé au code confidentiel personnel de l'émetteur et/ou du récepteur détenu par le service informatique (18) du centre de gestion (30) des télécopies.

5 5. Procédé selon les revendications 1, 2, 3 ou 4, comprenant en outre l'étape suivante :

- le centre de gestion (30) des télécopies émet à l'attention du récepteur (111 fig. 2) un avis de mise à disposition (190 fig. 2) d'une télécopie confidentielle.

10 6. Procédé selon les revendications 1, 2, 3, 4 ou 5, comprenant en outre l'étape suivante :

- un avis de relève (191) de la télécopie est adressé par le centre de gestion (30) des télécopies à l'émetteur (11).

15 7. Système permettant de transmettre une télécopie (162 fig. 1) de manière sûre entre un émetteur émettant la télécopie et au moins un récepteur (11 fig. 1) recevant la télécopie au moyen d'un télécopieur (161 fig. 1) associé à un équipement téléphonique (16 fig. 1) (ou à un terminal émulant cette fonction), les télécopies étant acheminées entre émetteur et récepteur par un réseau de communication (15) via un centre de gestion (30) des télécopies,

le dit système étant tel qu'il comprend :

20 - au moins une carte (10 fig. 1) à l'usage du récepteur (11 fig. 1), au format carte de crédit, personnalisée par des identifiants spécifiques à chaque carte et à chaque récepteur; la dite carte (10 fig. 1) comportant :

25 * des moyens d'émission (13 fig. 1) de brefs signaux acoustiques (20 fig. 1) d'identification, de type DTMF, actionnés (14 fig. 1) par le récepteur (11 fig. 1), au moyen d'un élément (14 fig. 1) accessible de l'extérieur de la carte (10 fig. 1),

* des moyens de cryptage permettant de crypter au moins en partie et de varier les signaux acoustiques chaque fois que la carte (10 fig. 1) est actionnée (14 fig. 1)

30 - un équipement téléphonique (16 fig. 1) (ou tout terminal émulant cette fonction) comprenant un microphone (17 fig. 1) destiné à recevoir et transformer les signaux acoustiques reçus, en des signaux électroniques transmis par le réseau de communication

(15) aux services informatiques (18) du centre de gestion (30) des télécopies,
- des moyens informatiques (21), associés aux services informatiques (18) du centre de gestion (30) des télécopies, connectés au réseau de communication (15), les dits moyens informatiques (21) comprenant :

5 * une base de données (23) contenant les références de chaque carte et de chaque récepteur et leurs données d'identification,

 * des moyens de traitement (24) et des moyens de comparaison (25) des signaux électroniques et des données d'identification contenues dans la base de données,

10 * des moyens d'émission de télécopie (28) émettant, en cas de coïncidence, à destination du télécopieur (161 fig. 1) du récepteur (11 fig. 1), la télécopie (162 fig. 1) qui lui est destinée par l'émetteur.

8. Système permettant de transmettre une télécopie de manière sûre entre au moins deux personnes, l'une, l'émetteur, (11 fig. 2) émettant la télécopie (162 fig. 2) au moyen d'un premier télécopieur (161 fig. 2), associé à un premier équipement téléphonique (16 fig. 2)
15) (ou à un premier terminal émulant cette fonction), l'autre, le récepteur (111 fig. 2), recevant la télécopie au moyen d'un second télécopieur (261 fig. 2) associé à un second équipement téléphonique (116 fig. 2) (ou à un second terminal émulant cette fonction), les télécopies étant acheminées par un réseau de communication (15) via un centre de gestion (30) des télécopies échangées entre émetteur et récepteur,

20 le dit système étant tel qu'il comprend :

- au moins deux cartes (10, 110 fig. 2), l'une à l'usage du récepteur (111 fig. 2), l'autre à l'usage de l'émetteur (11 fig. 2), au format carte de crédit, personnalisée par des identifiants spécifiques à chaque carte et à chaque émetteur ou récepteur ; la dite carte comportant :

25 * des moyens d'émission (13, 113 fig. 2) de brefs signaux acoustiques (20, 120 fig. 2) d'identification, de type DTMF, actionnés par l'émetteur ou le récepteur, au moyen d'un élément accessible (14, 114 fig. 2) de l'extérieur de la carte,

 * des moyens de cryptage permettant de crypter au moins en partie et de varier les signaux acoustiques chaque fois que la carte (10, 110 fig. 2) est actionnée (14, 114 fig. 2),
30

le dit système étant tel que :

- le premier et le second équipement téléphonique (16, 116 fig. 2) (ou le premier ou le second terminal émulant cette fonction) comprennent un microphone (17, 117 fig. 2) destiné à recevoir et transformer les signaux acoustiques reçus en des signaux électroniques transmis par le réseau de communication (15) aux services informatiques (18) du centre de gestion (30) des télécopies,

- des moyens informatiques (21), associés aux services informatiques (18) du centre de gestion (30) des télécopies, connectés au réseau de communication (15), les dits moyens informatiques (21) comprenant :

* une base de données (23) contenant les références de chaque carte et de chaque récepteur ou émetteur et leurs données d'identification,

* des moyens de traitement (24) et des moyens de comparaison (25) des signaux électroniques et des données d'identification contenues dans la base de données,

* des moyens de stockage (21a fig. 2) stockant, en cas de validation des identifiants de la carte de l'émetteur, la télécopie émise par le premier télécopieur,

* des moyens d'émission de télécopie (28 fig. 2) émettant la télécopie, à destination du télécopieur (261 fig. 2) du récepteur (111 fig. 2), en cas de validation des identifiants de la carte du récepteur.

9. Système selon les revendications 7 ou 8,

- la dite carte (10) comportant en outre :

* un compteur incrémental (105) interconnecté aux moyens d'émission (13) et aux moyens de cryptage (103), s'incrémentant d'au moins une unité chaque fois que la carte (10) est actionnée par l'élément (14),

de sorte que l'état du compteur incrémental (105) est émis à destination des moyens informatiques (21) et que les signaux acoustiques sont cryptés en fonction de l'état du compteur incrémental,

- les dits moyens informatiques (21) comportant en outre :

* des moyens de mémorisation (23, 230) de l'état $C(p,m)$ (246) du compteur incrémental (105) lors de la dernière opération validée,

* des moyens de comparaison (245) de l'état $C(p,n)$ (242) du compteur

incrémental (105) émis lors de l'opération en cours avec l'état $C(p,m)$ (246) du compteur incrémental mémorisé,

de sorte que la vérification de l'opération en cours est rejetée si $C(p,n)$ (242) est inférieur ou égal à $C(p,m)$ (246) et est poursuivie si $C(p,n)$ (242) est strictement supérieur à $C(p,m)$ (246),

- les dits moyens de traitement (24) et les dits moyens de comparaison (25) des signaux électroniques et des données d'identification contenues dans la base de données comportant des moyens permettant de recalculer (239) les signaux électroniques en fonction de l'état $C(p,n)$ (242) du compteur incrémental (105) et des données d'identification puis de les comparer (249) aux signaux électroniques transmis,

10. Système selon les revendications 8 ou 9, les dits moyens informatiques (21) comprenant en outre:

- des seconds moyens de comparaison (26) d'un code confidentiel personnel à l'émetteur ou au récepteur, contenu dans la base de données, à un code confidentiel personnel,

* émis par l'émetteur ou le récepteur, au moyen d'un clavier (27,127) associé au premier et/ou au second équipement téléphonique (16,116) ou à la carte de l'émetteur et/ou du récepteur,

* et transmis aux moyens informatiques (21) du centre de gestion des télécopies, par le réseau de communication.

11. Système selon les revendications 7, 8, 9 ou 10, tel que le centre de gestion des télécopies comprend en outre des moyens de délivrance (21b fig. 2), à destination du récepteur (111 fig. 2), d'un avis de mise à disposition (190 fig. 2) de la télécopie stockée.

12. Système selon les revendications 8, 9, 10 ou 11, tel que le centre de gestion des télécopies comprend en outre des moyens d'émission (29 fig. 2) d'un avis de relève (191 fig. 2) de la télécopie vers l'émetteur.

1/3

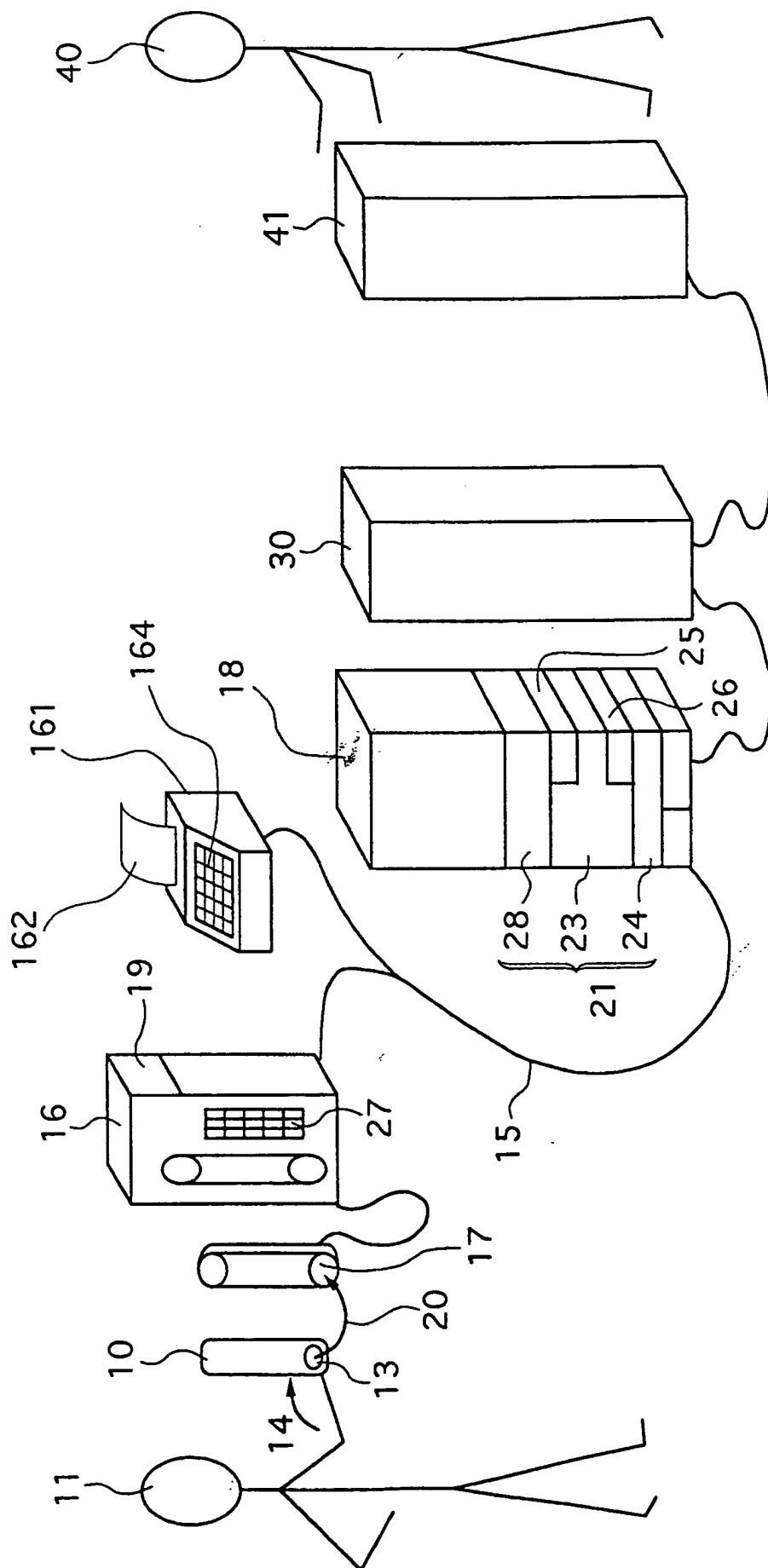
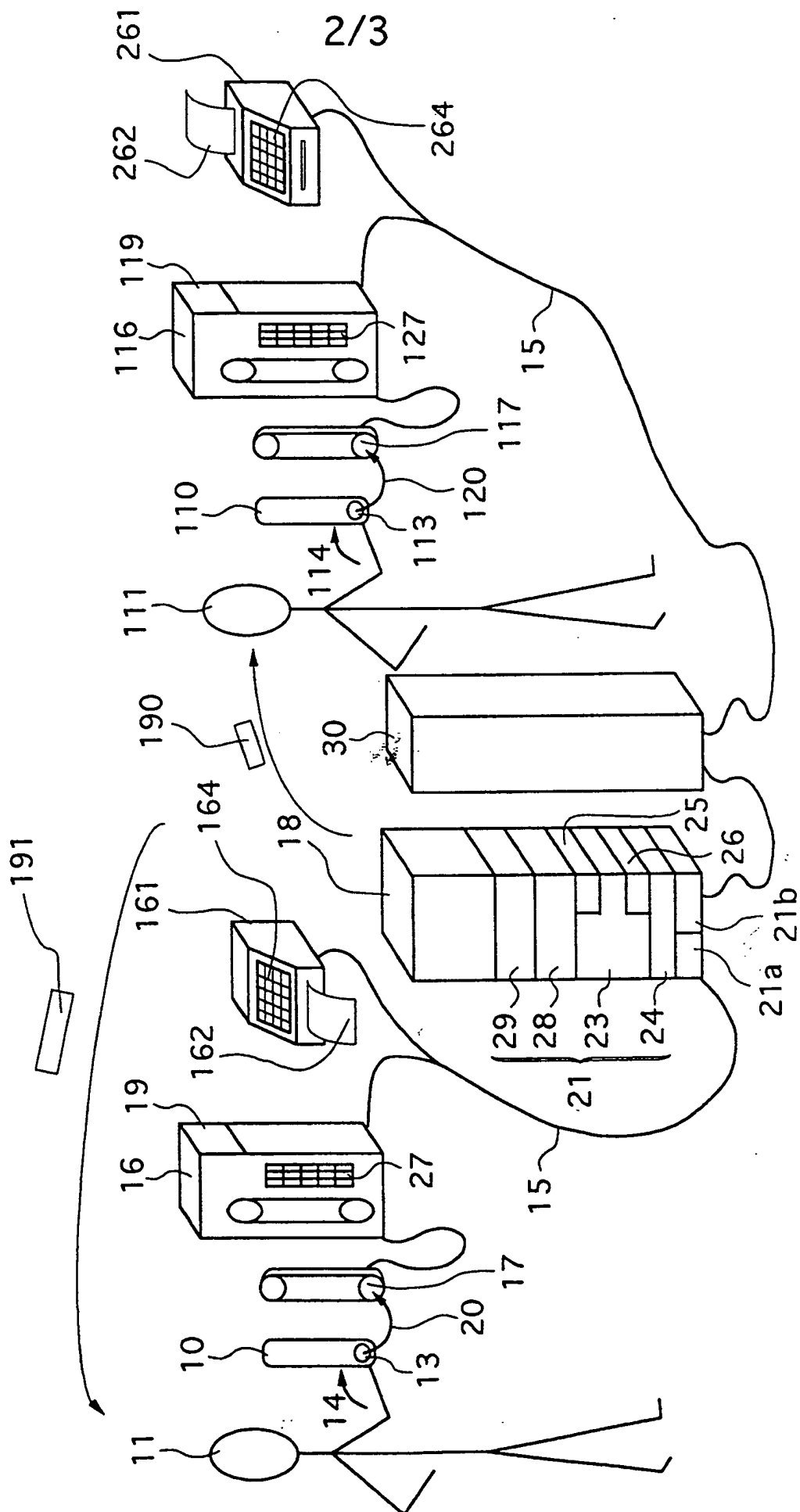


Fig. 1

Fig. 2

3/3

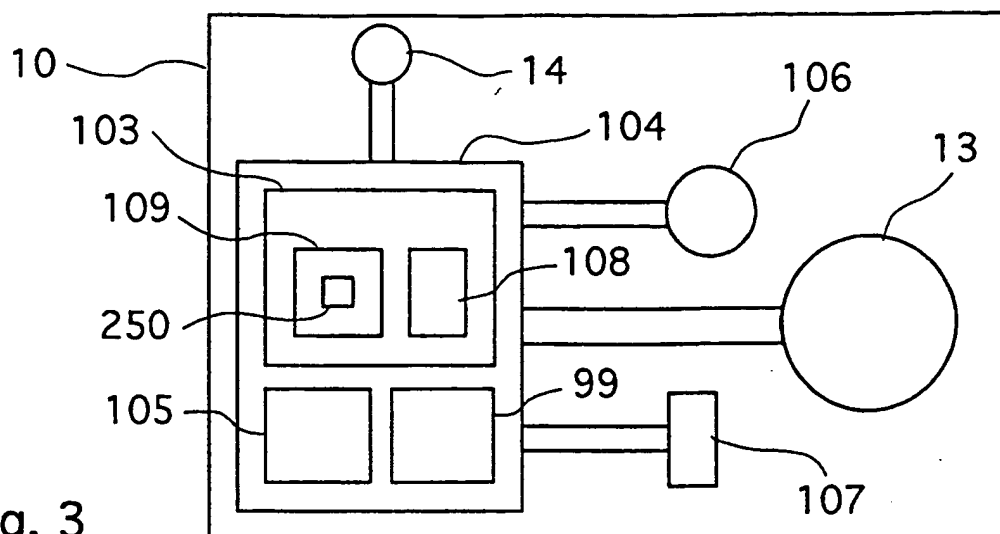


Fig. 3

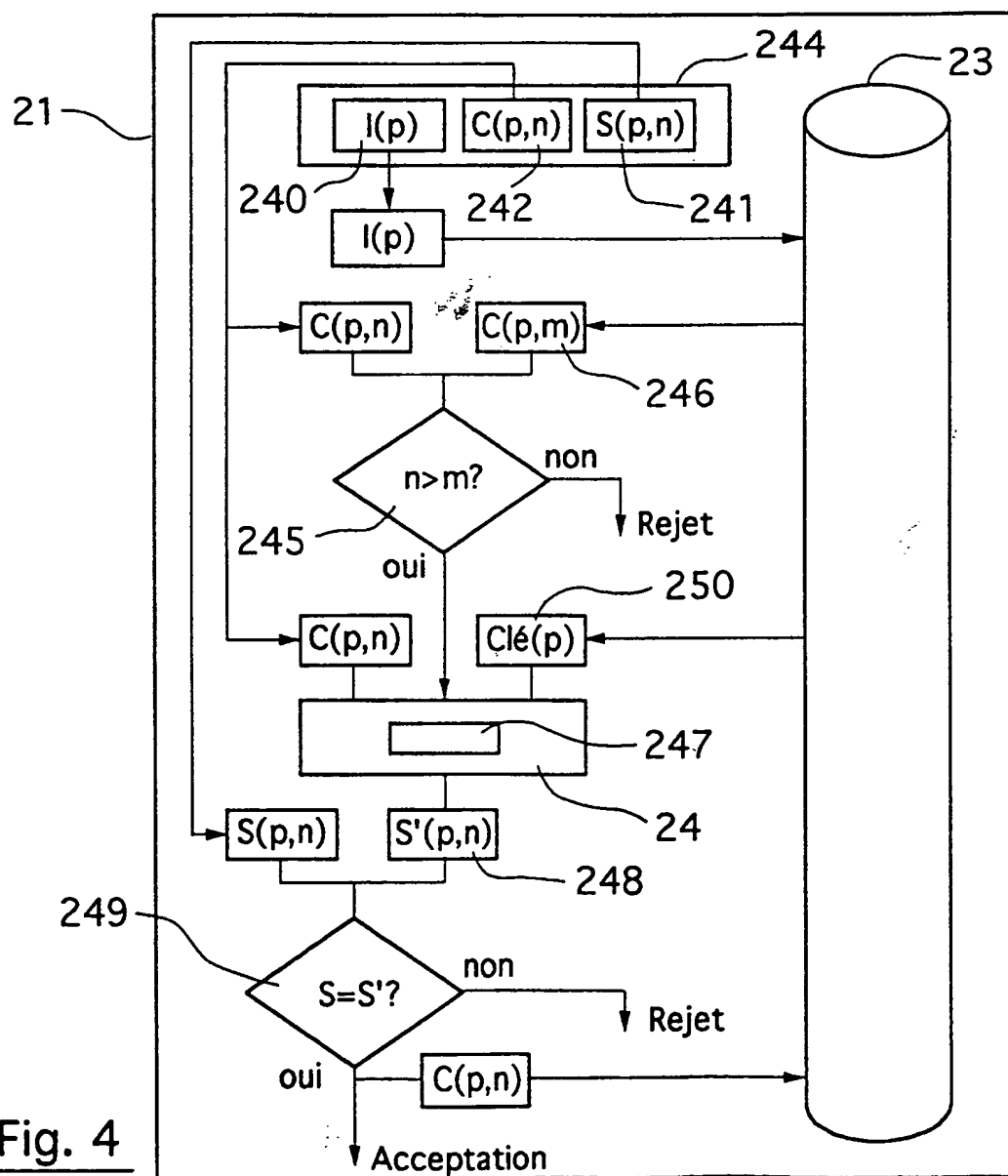


Fig. 4

INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR 97/01686

A. CLASSIFICATION OF SUBJECT MATTER

IPC 6 H04N1/44

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 360 732 A (R. J. GORDON) 28 March 1990 see column 13, line 65 - column 15, line 20 ---	1,2,4, 6-8,10, 12
Y	WO 96 04741 A (A. R. MARK) 15 February 1996 cited in the application see abstract see page 7, line 27 - page 8, line 2 --- -/--	1,2,4, 6-8,10, 12



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

20 January 1998

Date of mailing of the international search report

28/01/1998

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

De Roeck, A

INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR 97/01686

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	IEEE Global Telecommunications Conference, Globecom '92, Orlando, Florida, 6-9 December 1992; Conference Record, Vol. 2, 1992, IEEE pages 964-968 XP000357700 E.C.Chung et al.: "Implementation of a Fax Distribution System in the Local Area Networks of PCs" see page 966, right-hand column, last paragraph - page 967, right-hand column, line 22 ---	2,8
Y	EP 0 609 143 A (FRANCE TELECOM) 3 August 1994 see column 4, line 20 - line 22 ---	6,12
A	PATENT ABSTRACTS OF JAPAN vol. 12, no. 500 (E-699), 27 December 1988 & JP 63 211843 A (NEC CORP), 2 September 1988, see abstract ---	
A	EP 0 695 076 A (M. SERERO) 31 January 1996 -----	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 97/01686

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 360732 A	28-03-90	US 4994926 A CA 1329852 A JP 2192244 A US 5459584 A US 5291302 A	19-02-91 24-05-94 30-07-90 17-10-95 01-03-94
WO 9604741 A	15-02-96	US 5583933 A AU 3239795 A CA 2196784 A EP 0774189 A	10-12-96 04-03-96 15-02-96 21-05-97
EP 609143 A	03-08-94	FR 2700906 A JP 7046386 A US 5587809 A	29-07-94 14-02-95 24-12-96
EP 695076 A	31-01-96	FR 2722930 A	26-01-96

RAPPORT DE RECHERCHE INTERNATIONALE

De: le Internationale No

PCT/FR 97/01686

A. CLASSEMENT DE L'OBJET DE LA DEMANDE

CIB 6 H04N1/44

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 6 H04N

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	EP 0 360 732 A (R. J. GORDON) 28 mars 1990 voir colonne 13, ligne 65 - colonne 15, ligne 20 ---	1,2,4, 6-8,10, 12
Y	WO 96 04741 A (A. R. MARK) 15 février 1996 cité dans la demande voir abrégé voir page 7, ligne 27 - page 8, ligne 2 --- -/--	1,2,4, 6-8,10, 12



Voir la suite du cadre C pour la fin de la liste des documents



Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

1

Date à laquelle la recherche internationale a été effectivement achevée

20 janvier 1998

Date d'expédition du présent rapport de recherche internationale

28/01/1998

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

De Roeck, A

RAPPORT DE RECHERCHE INTERNATIONALE

Dern e Internationale No

PCT/FR 97/01686

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	<p>IEEE Global Telecommunications Conférence, Globecom '92, Orlando, Florida, 6-9 December 1992; Conference Record, Vol. 2, 1992, IEEE pages 964-968 XP000357700 E.C.Chung et al.: "Implementation of a Fax Distribution System in the Local Area Networks of PCs" voir page 966, colonne de droite, dernier alinéa - page 967, colonne de droite, ligne 22</p> <p>---</p>	2,8
Y	<p>EP 0 609 143 A (FRANCE TELECOM) 3 août 1994 voir colonne 4, ligne 20 - ligne 22</p> <p>---</p>	6,12
A	<p>PATENT ABSTRACTS OF JAPAN vol. 12, no. 500 (E-699), 27 décembre 1988 & JP 63 211843 A (NEC CORP), 2 septembre 1988, voir abrégé</p> <p>---</p>	
A	<p>EP 0 695 076 A (M. SERERO) 31 janvier 1996</p> <p>-----</p>	

RAPPORT DE RECHERCHE INTERNATIONALE

Derr e Internationale No

PCT/FR 97/01686

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 360732 A	28-03-90	US 4994926 A	19-02-91
		CA 1329852 A	24-05-94
		JP 2192244 A	30-07-90
		US 5459584 A	17-10-95
		US 5291302 A	01-03-94
WO 9604741 A	15-02-96	US 5583933 A	10-12-96
		AU 3239795 A	04-03-96
		CA 2196784 A	15-02-96
		EP 0774189 A	21-05-97
EP 609143 A	03-08-94	FR 2700906 A	29-07-94
		JP 7046386 A	14-02-95
		US 5587809 A	24-12-96
EP 695076 A	31-01-96	FR 2722930 A	26-01-96